The CRISP Project

- Distributed Intelligence in Critical Infrastructures -

Rune Gustavsson

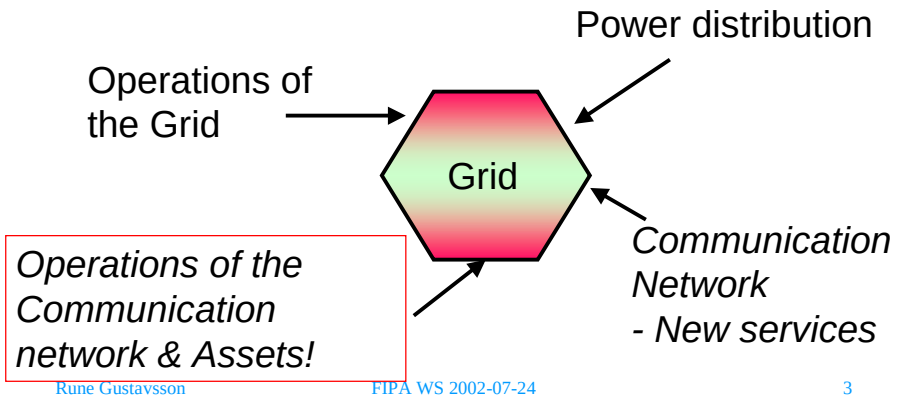
Department of Software Engineering and Computer Science (IPD)
Centre of Electronic Security (CES)
Blekinge Institute of Technology (BTH)

Presentation

- Setting the scene
- The CRISP project
- Sustainable information ecologies
- Coordination as computational markets
- Trustworthy systems
- Value of assets
- Summary

Security and utilities: Dependable systems

- Several perspectives. Vulnerabilities and threats increase the risks



Increasing numbers of security incidents

- Statistics from CERT Coordination Center (USA)

http://www.cert.org

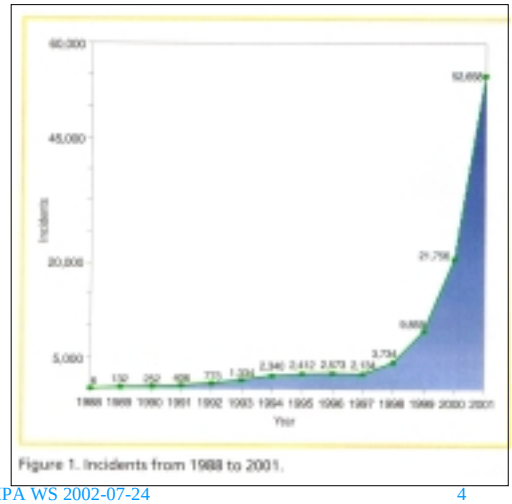


Figure 1. Incidents from 1988 to 2001.

Increasing number of vulnerabilities

http://www.cert.org

Vulnerability + Threat = Risk
Risk management crucial!

Due to
- **Increasing networking**
- **Increasing complexity of software**
- **Increasing 'user friend-liness'**
- **Lack of insights in 'Security Engineering'**
- **'Hidden affordances'**
- **More powerful adversaries**

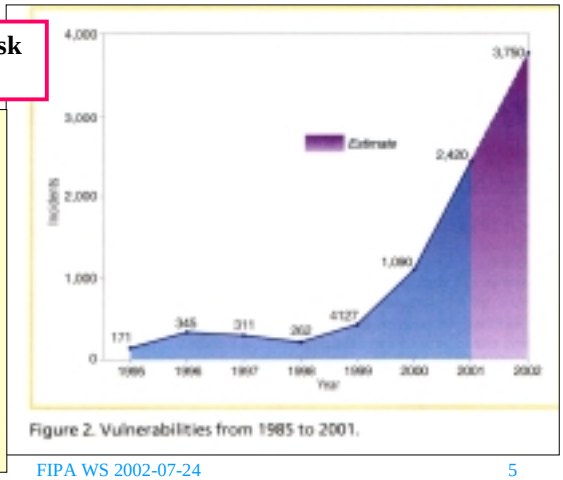


Figure 2. Vulnerabilities from 1985 to 2001.

Critical Infrastructures

- Joint efforts by US DoD and EPRI (Electric Power Research Institute)
  - *Complex Interactive Network/Systems Initiative*: "Secure and reliable operations of our energy and information infrastructures is fundamental to national and international economy, security, and quality of life"

Threats to power systems and society's other infrastructures

- **Attacks upon the power system**
  - Creating chaos by bring down electric supply
- **Attacks by the power system**
  - Ultimate target is the population using parts of the electricity infrastructure as a weapon (e.g., cooling towers to disperse chemical or biological agents)
- **Attacks through the power system**
  - Target is the civil infrastructures (e.g., electromagnetic pulse through the grid to damage computer or telecommunication infrastructures)

CRISP - Distributed Intelligence in Critical Infrastructures

- The CRISP project aims to investigate, develop and test how latest advanced intelligence by ICT technologies can be exploited in a novel way for cost-effective, fine-grained and reliable monitoring, management and control of power networks that have a high degree of Distributed Generation and RES penetration.
- The opportunities for interactive power networks create new possible control mechanisms that create flexibility and self-managing networks will be shown. Both normal and emergency operations are investigated covering different time scales. Insight in performance, security and architecture of highly distributed systems will be made available.
- Technical availability, functionality and economic cost-benefit considerations will be integrated.
- The results will contribute to better regional monitoring and control of local distribution in the EU-network.

The Consortium

P	Partner	Country	Main roles	WP leadership
P1	ECN	The Netherlands	Co-ordinator, project management, ICT specifications and development, demand-supply matching	WP II, WP V
P2	Eneco	The Netherlands	User aspects, experiment A	Tasks I.7, III.1-2A
P3	INPG/LEG	France	Development of simulation tools for fault detection, analysis and diagnostics, lab experiments	WP I, Task II.3
P4	Schneider	France	Electronics, system development, experiment B	Tasks III.1-2B
P5	EnerSearch	Sweden	E-market agent algorithms and architectures for power applications, exploitation manager	WP IV
P6	Sydkraft	Sweden	User aspects, evaluation of economics	Tasks I.2, III.3
P7	BTH	Sweden	Economics of network security models, intelligent agent architectures	Tasks I.6, II.4
P8	ABB	Sweden	Intelligent load shedding, experiment C	WP III, Task I.5

BTH Background

ISES Information/Society/Energy/Systems project 1996-98

- Subproject
  - Energy management through electronic markets
- International Industry and Academic consortium
  - Coordinator: EnerSearch AB

Other activities!

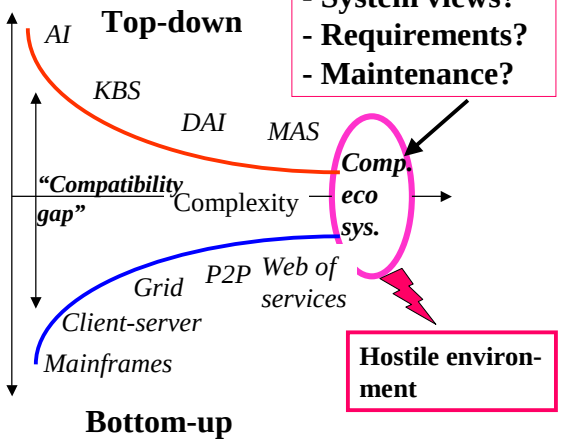
Related projects

- EC FET Alfebiite
  - Models of trust management in large information ecosystems
- VINNOVA project on Trustworthy Service Oriented Architectures
  - Cooperation with Kockums AB (Network Centric Warfare)
- SITI project on Sustainable Mobile Services in eHealthCare
- EC Network of Excellence (NoE)
  - AgentLinkII
  - Ontoweb
- EoI for 6FP
  - NoE*: European network on Coordination*
  - Integrated Project *IVA proposal: Secure Electronic Delegation & Integration : Ernst & Young, SICS, Telia, Ericsson, Electrolux, SignOn, CIT, LTH, LiU, BTH, IVA, IBS.*

Interesting Opportunities!!

Evolution of systems

- **Top-down cognitive approach**
  - AI
  - Multi Agent Systems
- **Bottom-up system abstraction approach**
  - Computers
  - Networks
  - Connectivity models



Methodologies!?
- System views?
- Requirements?
- Maintenance?

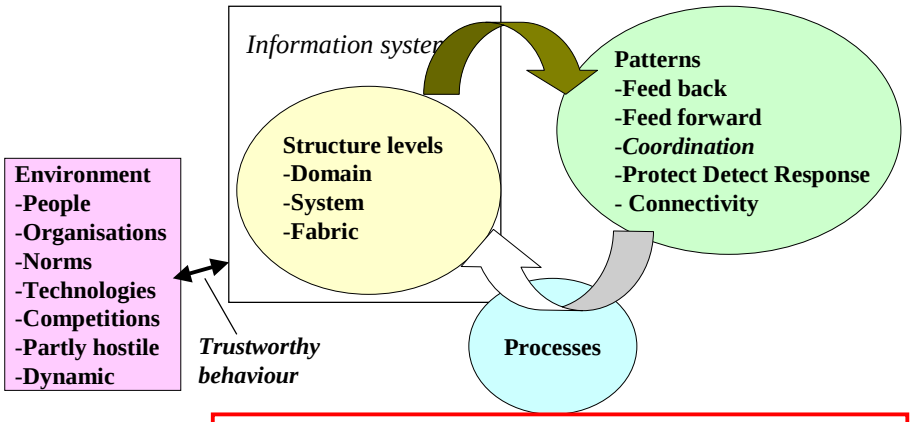
Hostile environment

Examples

- Complex adaptive systems
  - eHealth
  - *Safety critical infrastructures*
  - Network Centric Warfare
- New methodological approaches
  - Beyond simulations
  - Trusted dynamic delegation and trusted behaviour at breakdowns
  - Continuous observations and interactions supporting dynamic adaptations, information assurance, and shared cognitive awareness and decisions

A model of *open* computational systems

Main components of an information ecology



C.f. Varela-Maturana's model for living systems!

CONDENS Demonstrator

Conceptual demonstrator for network services

Stealth Vessel Visby Class

Domain and motivation

- Network-centric warfare.
- Service–oriented trustworthy distributed systems.
- Methodological principles of open computational systems.

Developed on our SOLACE Platform

Purpose and scope

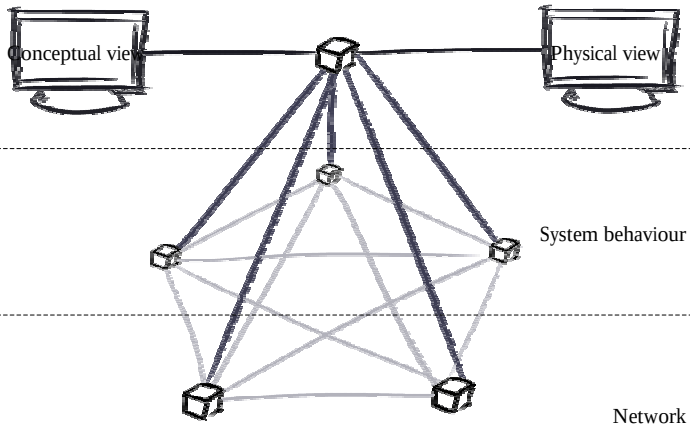
- **Quality** - Visualize the behaviour of autonomous entities under hostile and dynamic conditions (network-centric warfare scenario).
- **Sustainability** – Demonstrate system effectiveness, by means of dynamic behaviour, with respect to changing environment conditions.
- **Scalability** – Coordinate entities' behaviour by means of interaction in a distributed and dynamic network.

Together with Naval Shipyard Kockums AB - Howaldtswerke-Deutsche (HDW) AG (www.kockums.com)

CONDENS

- *Not* a simulation but an interface to complex systems -

QUALITIVE DOMAIN



SUSTAINABLE SYSTEMS

System behaviour

SCALABILE FABRIC

Network environment

Services

Services correspond to capabilities of entities.

Level

- Vessel hull (artifact)

Detonation

- Vessel explosives (artifact)

Mine hunt

- Vessel mine sweep capability (behavior)

Navigation

- Vessel propulsion capability (behavior)

Communication

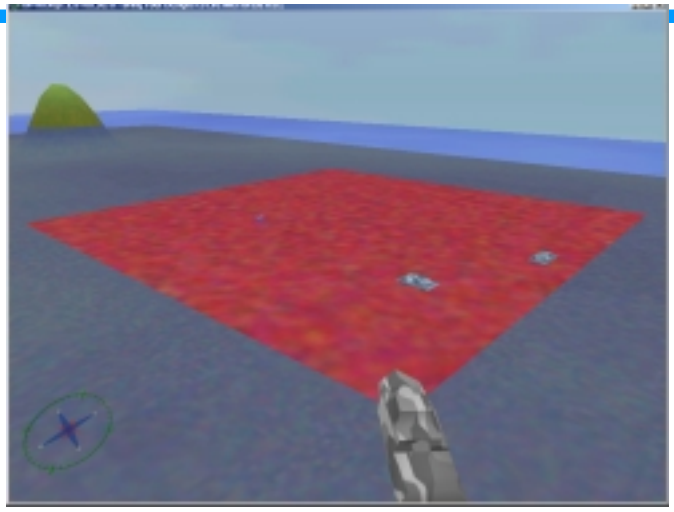
- Vessel interaction capability (behavior)

Sensor

- Vessel detection capability (behavior)

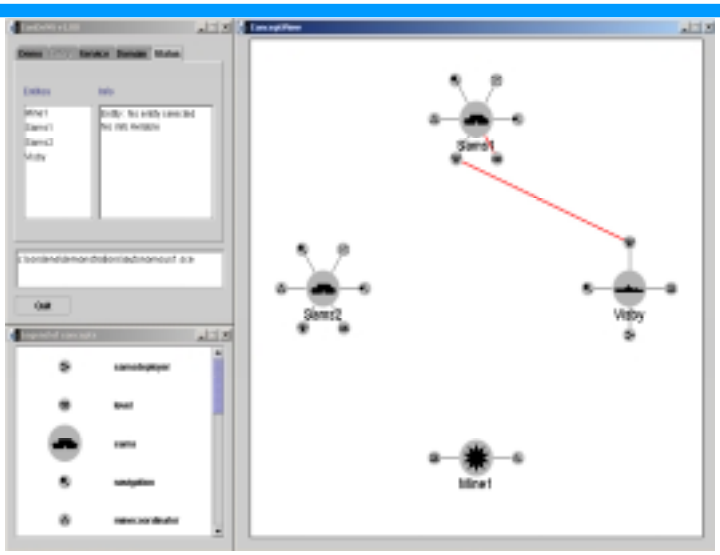
Physical system

- **SWEEP AREA**
- **MINES**
- **SAMS**
- **VISBY**



Conceptual system

- **ENTITIES**
- **SERVICES**
- **COMMUNICATION**



Rune Gustavsson

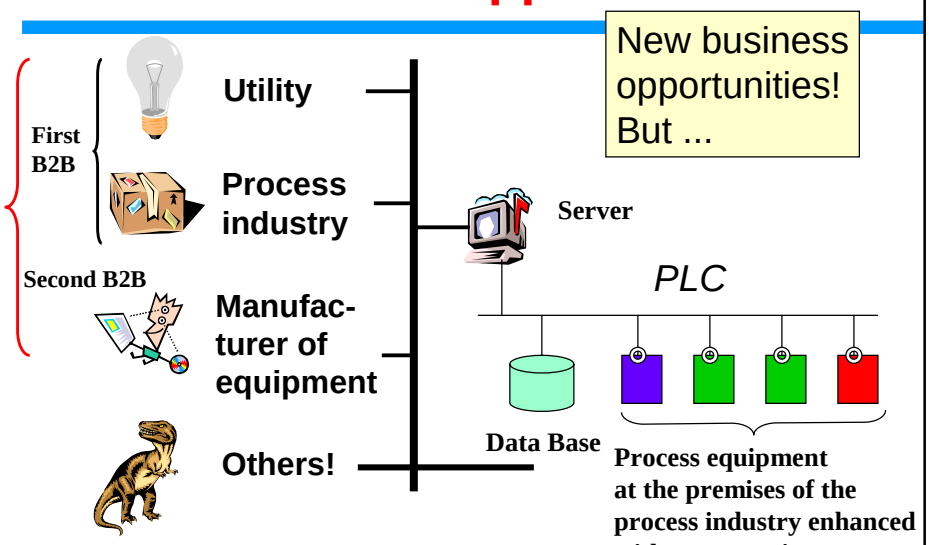
Summary of CONDENS

- **Quality** – By means of a separation between physical and conceptual views of system behaviour and local events, observation and construction of complex system behavior in network-centric settings is easier to comprehend.
- *However, qualitative aspects of system behavior must be complemented by means of a uniform tool for manual observation and construction. Furthermore, this tool must also be complemented with quantitative aspects of system behavior.*
- **Sustainability** – By means of a (cognitive) domain level, supported by SOLACE, dynamic system behavior can be effectively addressed.
- *However, dynamic system behavior must be complemented by means of continuous observation of new entities entering the system, i.e., not only dealing with situations where entities are removed from the system.*
- **Scalability** – By means of support for automatic network node coupling, a uniform interaction environment is created.
- *However, network node coupling must be complemented by means of more transport protocols as well as more efficient subnet-bridging.*

Trustworthy systems!

- Each of the business partners have to *trust* that even if the information is *shared* it can not be *misused*!
  - Infer secrets of others business processes.
  - Spy on other business processes.
  - Respect confidentiality and integrity of information.
- Each of the business partners have to *trust* that *vulnerabilities* inherent in networks will not transforms into threats and attacks by adversaries
  - Network security

A scenario: B2B application



Proposal: Two Frameworks

- A Framework protecting information. A combination of two classical models:
  - Bell-LaPadula: To protect *confidentiality*
  - Clark-Wilson: To protect *information integrity* and support auditing
- A Policy based Process model of security:
  - Combines *time dependence* of *Protection*, *Detection*, and *Response*.
  - A *comprehensive* model.

De-coupling and Affordances

- A crucial drawback of current technologies for web services is the *explicit coupling* of design-use as expressed in WSDL design description
  - Hampers service conjunction
    - *C.f. Openwings*
- The introduction of the structure component *Domain* allows us to de-couple the design-use pair into the triple design-use-affordances
  - C.f. Introduction of Knowledge Level in KBS

Smart web services

- A big technological challenge is support for *conjunction* of services. Conjunction of services is essential if we aim at re-use and re-combination as well as creating services from components
- A weak point of current use of WSDL, is the *implicit* assumption that there is *no* other view of a service than that given by the designer!
- To cover the whole lifecycle of a web service we have to *de-couple* the design and use into a service with a dynamic set of *affordances*
- This de-coupling, however also means that the repository services of publish and search have to be 'smart' or to have a semantic grounding
- A multi-agent approach allows us to introduce *active services* as well as *co-ordination support* in a principled way

Security issues!

XML + DAML + OIL

Supported by our SOLACE platform!

Sustainable systems

- A sustainable information *society* is a adaptable system that survives for some specified (non-infinite) time.
- Our goal is to develop a *comprehensive methodology supporting sustainable information societies*.

Sustainability invariance criteria

- *Sustainability* in information ecosystems can be recast in terms of criteria

Systemic properties

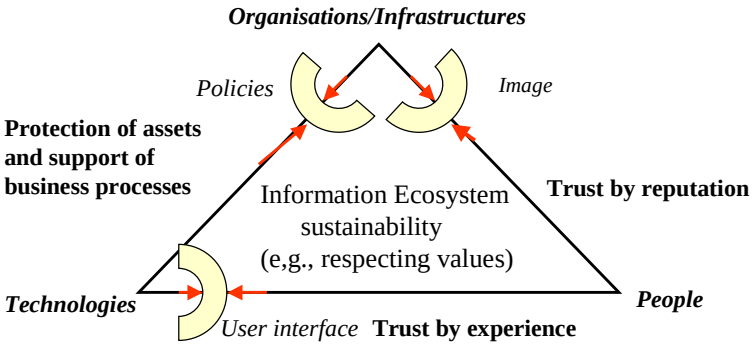
- Examples of Sustainability *invariance* criteria
  - *Trustworthiness*
  - *Profitability*
  - *Value preservation*
  - *Survivability*

Invariance is at the heart of our scientific understanding:
- Mathematics 'patterns and invariance'
- Physics 'conservative systems'
- Biology 'living systems'

N.B. Sustainability criteria are valid as long as external constraints does not create 'bifurcation situations' in the ecology!

Sustainable co-evolution

- An important sustainability mechanism is *sustainable co-evolution*
  - Critical interfaces



A Basic Set of Theories

- **Economic theories**
  - e³-Value
    - *Modelling profitability of value chains*
- **Risk management**
  - Economic risks
  - Assessing and safeguarding electronic assets
- **Ethnography and work practise**
  - Activity Theory
- **Software engineering**
  - Knowledge engineering; CommonKADS
  - Adaptive software development
- **Social and cognitive sciences**
  - Society and cognitive theories
  - Models of trust management
- **Complexity theories**
  - Autopoesis and dissipative systems (Complex Adaptive Systems)

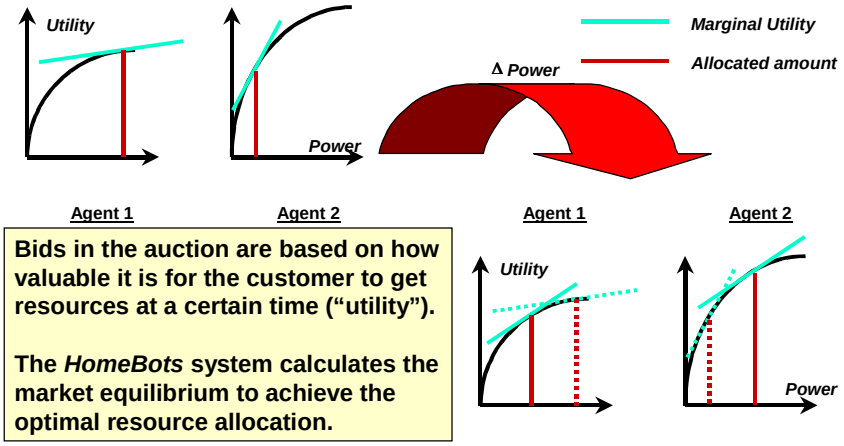
A common Framework is necessary for combining the different theories in a comprehensive and principled way

Smart distributed systems

- Distribution of 'intelligence'
  - Local control
- Global constraints
  - Limited resources
- Co-ordination
  - Flexible!
    - *Computational markets!*

Security issues related to auction based dialogues!?

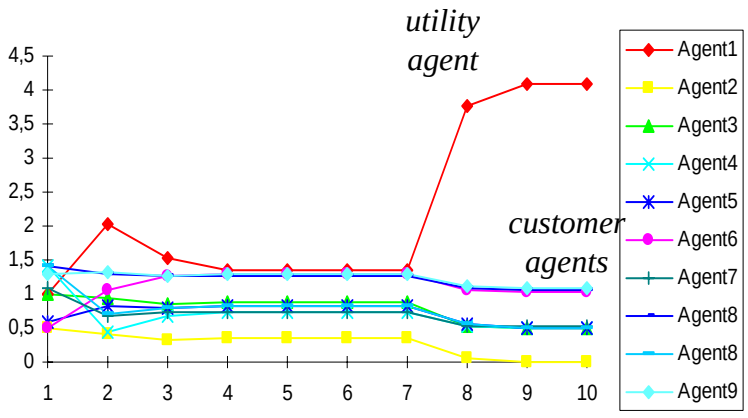
How does the electronic market work? - Economic utility theory



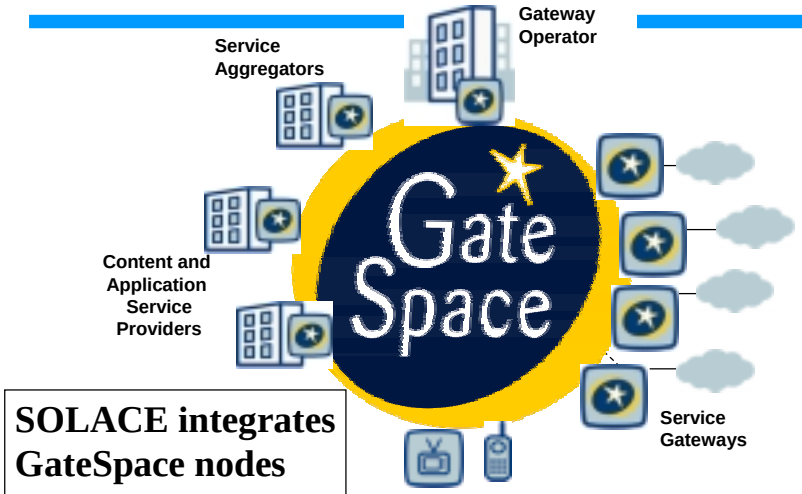
Bids in the auction are based on how valuable it is for the customer to get resources at a certain time ("utility").

The *HomeBots* system calculates the market equilibrium to achieve the optimal resource allocation.

Example: Dynamically Changing the Price



Gatespace's Distributed Service Platform



SOLACE integrates GateSpace nodes into a society

Why SOLACE and GateSpace?

- Extend OSGi functionality to support MAS
  - Lookup-/discovery service between and inside multiple gateways
  - Add support for service concepts on the community and society level
- Supports our 3-level system view
- Supports different architectures on the same hardware platform
  - Peer-to-Peer, client-server, Grid computing, mobile computing
- A common platform in several projects
- Strong industrial support!

E-Business Requirement Engineering

An e^3 - framework developed with VUA

- Feasibility model of business opportunities with several stakeholders
  1. Is the e-business idea at hand expected to be profitable for each actor involved?
  2. Are the supporting e-business information systems technically feasible?

Cost-benefit assessment of security investments!

Main features

- Different viewpoints
  - Business *Value* Viewpoint
  - Business *Process* Viewpoint
  - System *Architecture* Viewpoint
- Extension of ‘ Use Case Maps’
  - Scenario method for viewpoint integration
  - Iteratively progressing ‘spiral’ process of e-business requirements elicitation and analysis

Summary

- Due to the increasing complexity, in several senses, of networked dynamic systems we need to reassess current system thinking and software methodologies
- We suggest a holistic view on systems based on system theories in other disciplines, i.e., biology and natural sciences
- Furthermore we suggest a suitable methodology supporting systemic requirements, i.e, Information ecologies/societies and ecology invariants

Much work remains to be done! Not the least evaluations and extensions of our platform SOLACE